infoblox.

DEPLOYMENT GUIDE

Infoblox Integration with Checkpoint NGFW

Table of Contents

Introduction	2
Prerequisites	2
Known Limitations	3
Best Practices	3
Workflow	3
Infoblox Community Website Templates	4
Extensible Attributes	4
Session Variables	
Supported Notifications	5
List of Supported Notifications	5
Check Point Configuration	6
Enabling WAPI	
Creating API Only User	8
Creating Network Groups	
Infoblox NIOS Configuration	15
Verify Security Ecosystem is Installed	
Add/Upload Templates	
Modify Templates	17
Add a Rest API Endpoint	
Add Notifications	
Test the Integration	
Additional Resources	23

Introduction

The Outbound REST API integration framework from Infoblox provides a mechanism to create updates for both IPAM data (networks, hosts, leases) and DNS threat data into additional ecosystem solutions. Infoblox and Check Point's Next Generation Firewall (NGFW) enable security and incident response teams to leverage the integration of vulnerability scanners and DNS security to enhance visibility, manage assets, ease compliance and automate remediation. Thus, improving your security posture while maximizing your ROI in both products.

Prerequisites

The following is a list of prerequisites required for Outbound API notifications:

Infoblox:

- 1. NIOS 8.3 or higher
- 2. Security Ecosystem License
- 3. Outbound API integration templates
- 4. Prerequisites for the templates (e.g. configured and set extensible attributes)
- 5. Pre-configured required services: ADP, DHCP, Discovery, DNS, RPZ, and Threat Analytics
- 6. NIOS API user with the following permissions (access via API only):
 - All Network Views RW
 - All Hosts RW
 - All IPv4 Networks RW
 - All IPv6 Networks RW
 - All IPv4 Ranges RW
 - All IPv6 Ranges RW
 - All IPv4 DHCP Fixed Addresses/Reservations RW
 - All IPv6 DHCP Fixed Addresses/Reservations RW

Check Point Next Generation Firewall (NGFW):

1. Installed and configured Check Point NGFW

- 2. Access to the Check Point GAIA interface of the Check Point NGFW
- 3. Access to Check Point SmartConsole of the Check Point NGFW
- 4. User Credentials to the Check Point NGFW (User must be able to create and modify all Checkpoint Objects via the web interface.)

Known Limitations

Check Point's API will prevent updates to its database if another session is editing the same object elsewhere. Due to this, the Outbound API template publishes any and all changes to Check Point after a MODIFY, INSERT, or DELETE event occurs within the Infoblox device. Note that if CP_SecurityGroup or CP_AssetGroup are left open for editing or are modified without publishing in a different session, Check Point's API will not accept any changes or additions to those groups or objects.

Security events are statically assigned to the network group CP_SecurityGroup by the template. An administrator may need to flush devices that were placed in the aforementioned network group depending on the associated firewall rules and company policies.

Best Practices

As with most infrastructure changes to a production environment, it is recommended that a lab environment is utilized to test the functionalities and impact of any changes being made. Additionally, it is highly suggested to set the end point log level to Inform or higher (Warning, Error). Please refer to the NIOS Administration guide about other best practices, limitations, and any details on how to develop or modify notification templates.

Workflow

Use the following workflow to deploy this integration:

- 1. Properly configure Check Point to accept WAPI calls
- 2. Create an account for Check Point WAPI calls
- 3. Create the required Network Groups within CheckPoint's SmartConsole
- 4. Check that necessary services DHCP, DNS, RPZ and Threat Analytics are configured
- 5. Create Extensible Attributes
- Create or download the appropriate templates from the Infoblox community Website (<u>https://community.infoblox.com</u>): Check Point Assets, Check Point Security, Check Point Session, CheckPoint Login, Check Point Logout
- 7. Add/Upload Templates to Infoblox Grid

- 8. Add a REST API Endpoint
- 9. Add Notifications
- 10. Emulate an event, then check the debug log to verify changes on the REST API Endpoint

Infoblox Community Website Templates

Outbound API notification templates are an essential part of this integration. Templates enable Infoblox's Outbound API to automatically transfer data to Outbound endpoints based on notification configuration. Detailed information on how to develop templates is found within the NIOS Administrator guide. Infoblox does not distribute any templates with NIOS releases.

Templates are available on the Infoblox community Website. Templates may require additional extensible attributes, parameters, or WAPI credentials. Guidance on the required configurations are included with templates in the form of Deployment guides.

Extensible Attributes

Name	Description	Туре
CP_AddByHostName	Defines if Host records are to be added to Check Point by name.	List (true, false)
CP_AssetSync	Defines if syncing asset events with Check Point is desired or not.	List (true, false)
CP_AssetTimestamp	Timestamp that records when the asset was last synced with Check Point.	String
CP_SecuritySync	Defines if syncing security events with Check Point is desired or not.	List (true, false)
CP_SecurityTimestamp	Timestamp that is updated whenever a security event occurs.	String

Below is a table consisting of all extensible attributes utilized in this integration.

Session Variables

Below is a table consisting of all necessary Session Variables required for this integration.

Name	Description
CP_AssetGroup	The Asset Group is a Network Group located on the Check Point NGFW. All supported network objects that are populated from Infoblox are members of this group.
CP_SecurityGroup	The Security Group is a Network Group located on the Check Point NGFW. When a security event is triggered by a device, the device is added to this group.

Supported Notifications

A notification can be considered as a link between a template, an endpoint and an event. In the notification properties, you can define which events trigger the notification, the template to be executed, and the external endpoint. The Check Point Asset and Security templates support a variety of notifications. In order to simplify the integration, create the notifications listed in the table below and utilize relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed that is automatically populated by Threat Analytics. Modifying events that occur in real time will update the CP_AssetTimestamp on the associated object.

List of Supported Notifications

Notification	Description
DHCP Leases	DHCP Lease event
DNS RPZ	DNS query that is malicious or unwanted
DNS Tunneling	Data exfiltration that occurs on the network
Object Change Discovery Data	Device that is discovered on the network by Infoblox
Object Change Fixed Address IPv4	Fixed IPv4 address that is inserted, modified, or deleted
Object Change Fixed Address IPv6	Fixed IPv6 address that is inserted, modified, or deleted
Object Change Host Address IPv4	IPv4 host address that is inserted, modified, or deleted
Object Change Host Address IPv6	IPv6 host address that is inserted, modified, or deleted
Object Change Network IPv4	IPv4 Network that is inserted, or deleted
Object Change Network IPv6	IPv6 Network that is inserted, or deleted

Object Change Range IPv4	IPv4 Range that is inserted, modified, or deleted
Object Change Range IPv6	IPv6 Range that is inserted, modified, or deleted
Security ADP	ADP events that occur on the network

Check Point Configuration

Enabling WAPI

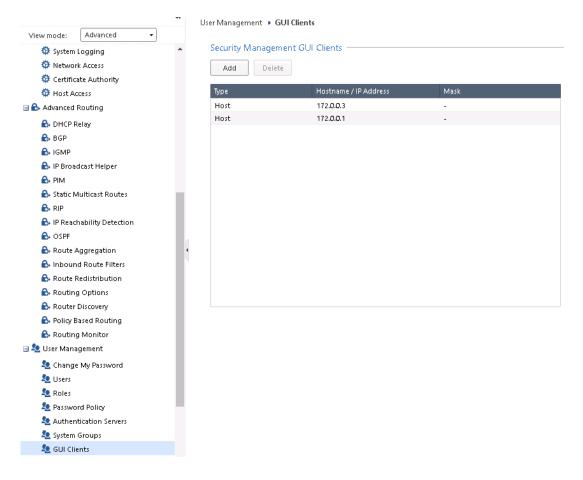
To Enable Check Point to accept inbound WAPI calls from Infoblox follow these steps:

1. (Optional)If you have not acquired the Check Point SmartConsole, please do so and install the program. On Gaia 2.6.18's network interface a light blue banner at the top contains a link to download the Check Point SmartConsole.

Manage Software Blades using SmartConsole 🛛 👽 Download Now! 🛛

Alternatively, you can download the SmartConsole from Check Point's website at <u>Check Point Support</u> <u>Center</u>. All SmartConsole screenshots will be from version R80.30. Please verify that you have the correct version that corresponds to your Check Point appliance.

 Access the GAIA interface of the Check Point appliance. Once inside, browse the left side panel and navigate to User Management → GUI Clients. Ensure that the Infoblox Grid Master's IP is added to the Security Management GUI Clients list. Additionally, you may want to add your current device to this list for testing purposes.



3. Log into the **Check Point SmartConsole** and click **MANAGE & SETTINGS** on the left side bar. Once inside, click on **Blades**, then **Advanced Settings...** under the **Management API** header. Inside the Management API Settings window, Click the **bubble** next to All IP addresses that can be used for GUI clients under the header Accept API calls from:. Before closing the dialog box, ensure that the Automatic Start setting under the header Startup Settings is checked and click **OK** to confirm all changes.

	**		
	🕨 🍄 Permissions & Administrat	General	
	III Blades	Global Properties Inspection Settings	
GATEWAYS & SERVERS	• 🖵 Sessions	nipecton occargini	
	🌣 Revisions 📃 🔽 .	Application Control & URL Filtering	
SECURITY	🥔 Tags	Advanced Settings	
POLICIES	🍄 Preferences	Auvanceu setungs	
	🗘 Sync with UserCenter	Content Awareness	
LOGS &		•	
MONITOR		Advanced Settings	
ö		Threat Prevention 3.	Management API Settings 🔍 🤤 🗙
MANAGE &		×	Startup Settings
SETTINGS		Advanced Settings	Automatic start
		Data Loss Prevention	··· Access Settings
	1.	Data Loss Prevention 4.	Accept API calls from:
		Configure in SmartDashboard 🕿	Management server only
			All IP addresses that can be used for GUI clients
		The second secon	All IP addresses
			OK Cancel
		Configure in SmartDashboard 🕿	Cancer
		•	7
		Compliance	
		Settings Inactive Objects	5.
		,	J.

4. Within the Check Point SmartConsole, Publish all changes by clicking **Publish** located on the banner.



5. Navigate back to the GAIA web interface and click the **Terminal** link on the top left of the banner.



6. Once inside the terminal, Log In, and input the command: API restart. This will finalize the changes made within the SmartConsole.

Terminal
login: admin
Password:
NGFW> api restart

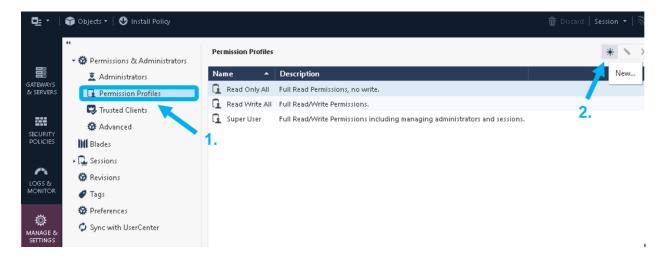
Creating API Only User

To add a user to Check Point that only has the ability to perform necessary API calls for this integration, follow these steps:

1. First create a **CheckPoint Permission Profile**. Within the Check Point SmartConsole, click on **MANAGE & SETTINGS** in the left side bar. Then, click on **Permissions & Administrators**.

⊡ : *	🗊 Objects 👻 😍 Install Policy					
	**	Admi	inistrat	ors		
	M Blades	Nam	e	Exp	iration Date	Profile
GATEWAYS & SERVERS	• 🕞 Sessions	ž :	admin	\odot	Dec 31, 2030	Super User
	🍄 Revisions 2.					
SECURITY	🖉 Tags					
POLICIES	🍄 Preferences					
~	🤣 Sync with UserCenter					
LOGS & MONITOR						
C MANAGE & SETTINGS	1 .					

2. Then click on **Permission Profiles** under the **Permissions & Administrators** header. Then, click the **New...** button within the Permission Profiles window.



 A New Profile dialog box will be revealed. Define a new name for the Permission Profile and customize the Permission Profile. Ensure all options are either deselected or are set to Write only. Only enable the following settings: • Write Common Objects. In the sidebar, click the Others option and ensure the Permission Profile has Write permissions for Common Objects.

New Profile		Q, 🔞 🛛 🗙
WAPI Us Enter Object		
•• Overview Gateways Access Control Threat Prevention Others Monitoring and Logging Events and Rep. rts Management Endpoint	Permissions Common Objects 2. Check Point Users Database LDAP Users Database User Authority and Access HTTPS Inspection Client Certificates User and Device Management Configuration	Write Read
	OK	Cancel

o Management API Login. In the sidebar, click the Management option and ensure that the checkbox next to Management API Login is checked. Once completed click OK.

Profile	୯ ଡ ଼ା ×
WAPI Us Enter Object O	
 Overview Gateways Access Control Threat Prevention Others Monitoring and Logging Events and Reports 	Management Permissions Manage Administrators Manage Sessions High-Availability Operations Management API Login 2.
Management Endpoint	
1.	Add Tag OK Cancel

4. Now create an Administrator account for the integration. Click on the **Administrators** option under the **Permissions & Administrators** header. Then within the Administrators window, click **New...** A New Administrator dialog box will be revealed.

	≪ ▼ ✿ Permissions & Administrators	Administra	tors				* 1
	Z Administrators	Name	Expiration Date	Profile	Authentication Method	Locked	Ne
SATEWAYS & SERVERS	Permission Profiles	🚊 admin	⊙ Dec 31, 2030	Super User	OS Password		
	🔛 Trusted Clien						
SECURITY	🏶 Advanced						2.
POLICIES	III Blades						
	🕨 🖵 Sessions						
- ^^ .065 &	🍄 Revisions						
MONITOR	🥔 Tags						
	🍄 Preferences						
ن MANAGE & SETTINGS	🧔 Sync with UserCenter						

5. Give the New Administrator a name. note, this is the user account that will be used for the outbound endpoint later demonstrated later in this guide.

New Administrator			Q,	?	×
	ioblo: ter Object Comment				
44	A 10 10 10				
General	Authentication				
Additional Info	Authentication Method:	Check Point Password 🔹			
	🛇 Password is not defined *	Set New Password			
	Certificate Information:				
	🛇 Certificate is not defined	Create			
	Permissions				
	Permission Profile: *	No item selected.	-	•	
	 Expiration Never Expire At: 9/24/2021 				
	🖉 Add Tag				
		ОК	Cancel		

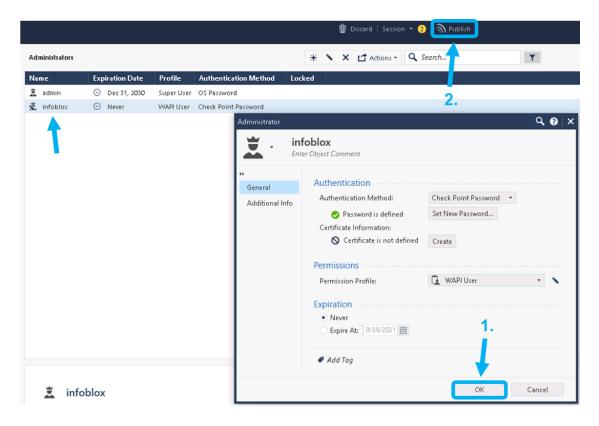
6. Select the **Permission Profile** that was created in steps 1 through 3 by clicking the **dropdown** menu next to Permission Profile: and selecting a profile.

New Administrator			٩	•	<
• •	foblox er Object Comment				
•• General Additional Info	Authentication Authentication Method: Password is not defined * Certificate Information: Certificate is not defined	Check Point Password Set New Password Create	•	1.	
	Permission Profile: * Expiration • Never Expire At: 9/24/2021	No item selected.	- New	•	
		4 items available OK	.:i Cancel		

7. Define a new password for the New Administrator by clicking on **Set New Password**.... Ensure that the checkbox next to "U**ser must change password on next login**" is not checked. Click **OK** on the Set Password dialog box when complete.

	foblox er Object Comment		
** General	Authentication		
Additional Info	Authentication Method:	Check Point Password 🔹	Set Password X
	 Password is not defined * Certificate Information: Certificate is not defined Permissions	Set New Password Create 3.	Password: ••••• Confirm: ••••• User must change password on next login
	Permission Profile:	🔂 WAPI User	OK Cancel
	Expiration Never Expire At: 9/24/2021		4.

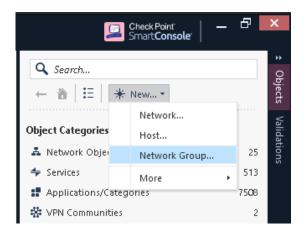
8. Click **OK** to complete the New Administrator creation. A new Administrator account should be visible in the Administrator window. To finalize the creation of the Administrator, click **Publish** located on the top center of the SmartConsole screen, and Publish all changes.



Creating Network Groups

To add the necessary Network Groups to Check Point, follow these steps:

1. Once logged into the Check Point SmartConsole, expand the tab labeled **Objects** in the top right of the window. Inside the Objects pane click **New...**, and select **Network Group...**.



2. Name the new Network Group CP_AssetGroup. Click **OK** to finish making the Network Group. *Please note that Network Groups are case-sensitive.*

New Network Gr	oup		९, 🕑 🗖 ×
	CP_AssetGroup Enter Object Comment		
+ ×		Q Search	
Name	 IP Address 	Mask	Comments
	No iter	ms found	
🥔 Add Tag			
		ОК	Cancel

3. Repeat step 2 to create the Network Group: CP_SecurityGroup. Once added, click **Publish** on the top banner to finalize the making of both Network Groups.



 To verify that both Network Groups were created navigate to Network Objects → Groups in the Objects pane. If done properly, you will see CP_AssetGroup and CP_SecurityGroup under the Network Groups header.



Infoblox NIOS Configuration

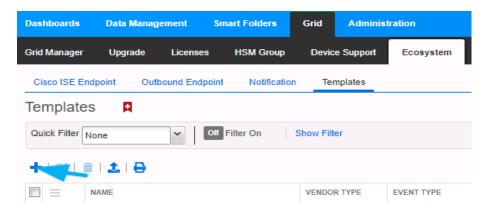
Verify Security Ecosystem is Installed

The Security Ecosystem license is a Grid Wide license. Grid wide licenses activate services on all appliances in the associated Grid. To check if the license is installed navigate to Grid \rightarrow Licenses \rightarrow Grid Wide.

Dashboards	Data Manag	jement	Smart Folders	Grid
Grid Manager	Upgrade	Licenses	HSM Group	Devic
Licenses	A			
Member	Pool Grid	Wide		
Quick Filter	None	•	Off Filter On	Show F
+ = 3	e 14			
	FEATURE 🔺		LIMIT CONTEXT	
	RPZ			
	Security Ecosys	ter		

Add/Upload Templates

 In order to add or upload templates, navigate to Grid → Ecosystem → Templates and click on the + or + Add Template button in the right-side Toolbar.



2. In the Add Template window click the Select button next to Filename:.

Add Template	5	×
Filename:	Select	@ 《
Close		View Results Add

3. In the Upload window click **Select** and locate the CheckPoint Login.json template.

Upload		×
File	Select	Q Wpload
Close		

4. Once the path of the CheckPoint Login.json file is populated in the File text field, click the **Upload** button.

Upload	i		×
File	C:\fakepath\Check Point Login.json	Select	Q K Upload
Close			

5. Click **Add** to complete the operation.

Add Template		×
Filename: Check Point Login.json	Select	@ «
Close		View Results Add

6. Verify that the CheckPoint Login.json template has been added within $Grid \rightarrow Ecosystem \rightarrow Templates$.



7. Repeat steps 1 through 5 with all required templates. The following templates are required: Check Point Assets, Check Point Security, Check Point Session, CheckPoint Login, and Check Point Logout.

Modify Templates

NIOS provides the ability to modify templates via the web interface.

- 1. Navigate to Grid \rightarrow Ecosystem \rightarrow Templates and click on the \equiv hamburger icon next to the template you want to modify. Click the Edit button to open the Template window.
- 2. The template editor is a simple interface for making changes to templates. It is recommended to only use the template editor to make minor changes. You can also edit, cut, and paste template snippets from a text editor. Please note that you cannot delete a template if it is used by an endpoint or by a notification.

CheckPoint Assets (Tem	plate)	×
	Basic	8
General Contents	<pre>{ "name": "CheckPoint Assets", "comment": "Check Point Asset Template for NIOS 8.4 Outbound API", "version": "5.0", "type": "REST_EVENT", "event type":["DISCOVERY_DATA", "FIXED_ADDRESS_IPV6", "FIXED_ADDRESS_IPV6", "HOST_ADDRESS_IPV6", "HOST_ADDRESS_IPV6", "LEASE", "NETWORK_IPV6", "RANGE_IPV4", "RANGE_IPV4", "RANGE_IPV6", "content_type": "application/json", "vendor_identifier": "Check Point", "dustion", "Xucha", "headers": {{</pre>	《
	"operation": "NOP", "body": "\${XC:DEBUG;{H:}}\${XC:DEBUG;{E:}}\${XC:DEBUG;{L:}}\${XC:DEBUG;{L:}}\${XC:DEBUG;{L:}}\${XC:DEBUG;{L:}}\$ /< \\$ <	k ↓
Cancel	Save & Clo	se 🔻

Add a Rest API Endpoint

REST API Endpoints are remote systems that receive changes based upon notifications and configured templates. A Grid, for example, can not only send notifications, it can also receive the notification from itself for varying purposes.

1. To add a REST API Endpoint, navigate to Grid → Ecosystem → Outbound Endpoint and click the + icon, then click the Add REST API Endpoint button.

Dashboards	Data Manag	ement Sm	art Folders	Grid	Administ	ration
Grid Manager	Upgrade	Licenses	HSM Group	Devic	e Support	Ecosystem
Cisco ISE End	lpoint Out	bound Endpoint	Notificatio	n Ter	nplates	
Outbound	Endpoint	A				
Quick Filter N	one	✓ Off	Filter On	Show Filt	er	
+ - 🗹	💼 🕹 🖨					
Add RES	T API Endpoint	ENDPOINT T	YPE URI			VENDOR TYPE
Add DXL	Endpoint	DEAT OF				a

- 2. The Add Rest API Endpoint Wizard will open. URI and Name are requirements when configuring an endpoint. Input the following information:
 - o Enter a name you will recognize and the complete URI of the device (Example: https://172.0.0.9)
 - o Specify **Auth Username**, **Auth Password** (Check Point credentials, Creation of user account demonstrated on pg. 9)
 - o WAPI Integration Username and WAPI Integration Password (NIOS credentials). Once complete, Click Next

Add REST API Endpoin	nt Wizard > Step 1 of 3	×
*URI	https://172.0.0.9	^ 0 «
*Name	Check Point	
Vendor Type	Check Point	
Auth Username	Test	
Auth Password	Clear Password	
Client Certificate	Select Clear	
WAPI Integration Username	Test	
WAPI Integration Password	Clear Password	
Server Certificate Validation	Use CA Certificate Validation (Recommended) CA Certificates Enable Host Validation	-
Cancel	Previous Next Save	& Close 🔻

- 3. Be aware that the Test Connection function only checks communication (establishes TCP connection with a remote system) with the URI. It does not check the authentication credentials.
- 4. It is recommended to send notifications from a Grid Master Candidate if there is one available as an alternative to the Grid's Grid Master.
- 5. Under Step 2 of the Add REST API Endpoint Wizard, set the Log Level to Debug for debug purposes during initial configuration. Additionally, click the **Select Template** button to populate the correct Session Template. When complete, click **Save & Close**.

Add REST API E	ndpoint Wizard > Step 2 of 3	×
Timeout Log Level Template Vendor Type Template Type Parameters	30 Seconds Debug ▼ Check Point Session Select Template Check Point Session Management	
NAME	VALUE TYPE	
CP_AssetGroup	AssetGroup String	•
Cancel	Previous Next	Save & Close 🔹

Add Notifications

A notification is a link between a template, an endpoint, and an event. In the notification you define the event which triggers the notification, executed template, and the API endpoint of which the Grid will establish a connection. The Check Point templates on the Infoblox community Website support all available notifications.

To simplify the deployment of this integration, create only desired notifications and use relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed automatically populated by Threat Analytics. Note: when testing notifications using Test Rule, rules for that notification apply.

In order to add a Notification a Template must be added. To add a Notification, follow these steps:

 Navigate to Grid Ecosystem → Notification and click the + above the list of notifications or + Add Notification Rule button on the right-side Toolbar. This will reveal the Add Notification Wizard.

Dashboards	Data Managem	ent Smart	t Folders	Grid	Administration				Q Search	admin
Grid Manager	Upgrade I	Licenses H	HSM Group	Device St	upport Ecosy	vstem				
Cisco ISE Endp	oint Outbou	nd Endpoint	Notification	1 Templa	ates			Toolbar		≫
Notification							+ Add Notification Rule			
Quick Filter Not	ie	▼ Off Filt	er On	Show Filter				🗹 Edit 🛅 Delete		
+ © =	e					Go to	Go	≓ IDN Con	verter	
	AME 🛋	TARGET	ACTIO	N	DISABLED					

2. Once inside the Add Notification Wizard, enter a **Name** in the Name text box to identify the notification type. Next, click **Select Endpoint**. Then, Put a relevant comment in the Comment text box if desired. Finally, click the **Next** button.

*Name CP_Host_IPv4 *Target Check Point Select Endpoint Notification rules will be reset when you change the endpoint type. Target Type REST API Vendor Type Check Point Comment Disable	Add Notification W	/izard > Step 1 of 4	×
Target Type REST API Vendor Type Check Point	*Name	CP_Host_IPv4	^ @ «
Target Type REST API Vendor Type Check Point Comment	*Target	Check Point Select Endpoint	
Vendor Type Check Point Comment		Notification rules will be reset when you change the endpoint type.	
Comment	Target Type	REST API	
	Vendor Type	Check Point	
Disable	Comment		
Disable			
		Disable	
Cancel Previous Next Save & Close -	Cancel	Previous	▼ Save & Close ▼

3. Click **Next**, select an Event type, by using the Event dropdown. Define one or many rules via the Filter and Operator dropdowns under the Match the following rule: header. Rules act as filters that decide if a template should be executed or not. To add additional rules, click the + button next to an existing rule. When more than one rule is present, a dropdown will populate allowing for the choice of All or Any defining the logic required before the associated action is executed. Note: for optimal performance, it is best practice to make the rule filter as specific as possible.

Add Notification Wizard > Step 2 of 4								
It may take up to a minute to	apply the new rules.			8 «				
*Event Object Change Host Address IPv4 T								
Match the following rule:			Reset					
Network	▼ equals	▼ 172.0.0.0/24						
Cancel	Pre	vious	Save & Close	•				

4. Click **Next** until Step 4 of the Add Notification Wizard is reached. Then, click the **Select Template** button to populate a relevant template that will be executed if the notification is triggered. Finally, click **Save & Close** to complete the creation of the notification.

Add Notification Wizard > Step 4 of 4							×
*Template Vendor Type Template Type Parameters	CheckPoint Check Poir Event	Select template	Clear			•	8 «
NAME		VALUE		TYPE			
No data Cancel		Previous	Next		Save & Cl	• ose	•

5. (Optional) Repeat steps 1-4 to add additional rules depending on your needs.

Test the Integration

You can now test any notifications that you have made by emulating events via the Test Rule function. Testing a rule will show you if the implementation of a template is correct, and what steps the Outbound Endpoint takes when performing an Outbound API call.

1. (Optional) Clear the Debug Log by navigating to Grid \rightarrow Ecosystem \rightarrow Outbound Endpoint. Select the \equiv hamburger icon next to the relevant Outbound Endpoint and click Clear Debug Log.

Test a notification, by navigating to Grid → Ecosystem → Notifications. Once there, click on the = hamburger icon next to a notification and click Test Rule. This will reveal a Test Rule window.

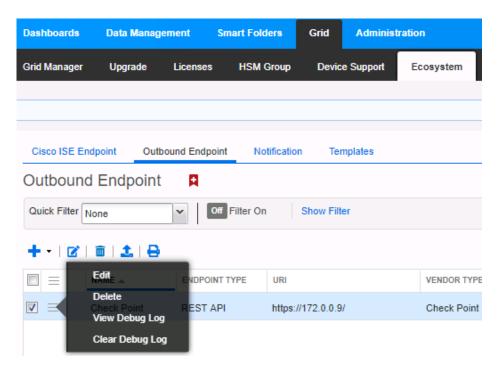
Dashboards	ashboards Data Manageme		ent Smart Folders		inistration	stration	
Grid Manager	Upgrade	Licenses	HSM Group	Device Suppo	ort Ecosy	stem	
Cisco ISE End	dpoint Outb	ound Endpoint	Notification	Templates			
Notificatio	n 🖪						
Quick Filter	one	V Off F	Filter On S	how Filter			
+ & =	i 🖨						
	Edit	TARGET	ACTION		DISABLED		
	Delete CP_ADP Test Rule	Check Poin	t Outbou	ind Template	No		
	View Debug Log	Check Poin	t Outbou	ind Template	No		
	CP_Fixed_IPv4	Check Poin	t Outbou	ind Template	No		
	CP_Fixed_IPv6	Check Poin	t Outbou	ind Template	No		
	CP_Host_IPv4	Check Poin	t Outbou	ind Template	No		

3. You can modify test events within the Test Rule window. To perform the test function, click the **Test** button. If the test was successful you should see a Success message near the top of the window. If the test has failed there is likely a syntax error, or there are incorrect parameters for the Test.

Test Rule	×
<pre>Parameters { "rule_severity": "MAJOR", "event_type": "ADP", "timestamp": "2019-09-17T119:27:392", "vnode_oid": 0, "rule_name": "Blacktsis:10.0.0.1", "sequence_id": 0, "member_name": "nios.poc.infoblox.local", "thread_id": 0, "nule_category": "BLACKLIST DROP UDP IP prior to rate limiting", "rule_ation:" 'DROP", "rule_sid": "120103001", "source_jp:": "10.0.0.1", "source_port: 49736, "query_fgdn": "*.domain.com" } </pre>	▲ ② ≪
Close	Test

4. Once the Test Rule function has been executed, view the Debug Log. This is done by navigating to Grid → Ecosystem → Notifications and clicking on the = hamburger icon next to a relevant notification and selecting View Debug Log. Alternatively, you can view the Debug Log by navigating

to Grid \rightarrow Ecosystem \rightarrow Outbound Endpoints and clicking the \equiv hamburger icon next to the relevant Outbound Endpoint. Please note that debug logs may be downloaded locally or be blocked by an ad blocker.



Additional Resources

Infoblox Community

Infoblox NIOS Documentation

Check Point CheckMates

Check Point Management API Reference

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters 2390 Mission College Blvd, Ste. 501 Santa Clara, CA 95054 +1.408.986.4000 www.infoblox.com

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).